UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,956	05/09/2001	David Carroll Challener	RPS9 2001 0022	4042

45211 7590 08/21/2007

Robert A. Voigt, Jr.
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER	
NGUYEN, NGA B	

ART UNIT	PAPER NUMBER
3692	

MAIL DATE	DELIVERY MODE
08/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/851,956
Filing Date: May 09, 2001
Appellant(s): CHALLENER, DAVID CARROLL

Robert A. Voigt, Jr. (Reg. No. 47,159)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on March 27, 2007 appealing from the Office action mailed October 19, 2006.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The statement of the status of Amendments contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of invention contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The summary of the ground of rejection to be reviewed on appeal contained in the brief is correct.

(7) Claim Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence relied Upon

"Trusted Computing Platform Alliance (TCPA)", Main Specification Version 1.0, January 25, 2001, pp.1-284.

(9) Grounds of Rejection

The following grounds of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trusted Computing Platform Alliance (TCPA), TCPA Design Philosophies and Concepts, Version 1.0.

Regarding to claims 1-2, TCPA discloses a method and a computer program product adaptable for storage on a computer readable medium, comprising the steps of (see the entire document, pages 1-30):

a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer (*see page 9, 2.5.1, the TPM contains a private endorsement key, the Owner makes available the endorsement credential the platform credential and the conformance credential*), and a second certificate acquired by the computer system from a Certification Authority (CA) (*see page 7, 2.4.1.1 and 2.4.1.2, the CA enables determination of the identity of an entity by providing a certificate that binds the identity label of an entity*);

creating a public/private key pair and a third certificate in response to the receiving step (*see page 8, 2.4.1.7*); and

sending the public/private key pair and the third certificate to the customer over

the network (*see page 10*).

TCPA does not disclose receiving from a customer over a network an application for a credit card authorization and the customer is capable of using the public/private key pair and the third certificate to make purchases over the network. However, Official Notice is taken that receiving from a customer over a network an application for a credit card authorization and the customer is capable of using the public/private key pair and the third certificate to make purchases over the network are well known in the art. For example, the conventional electronic commerce allows the user purchases products over the Internet using a credit card, the user submits purchase request include credit card information, the credit card information is then transmitted to the credit card company for verifying and authorizing the purchase request. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to apply the method of TCPA above for the purpose improving the security in purchasing products using credit card over the Internet.

Regarding to claims 3-5, TCPA further discloses wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity, wherein the third certificate is associated with an endorsement key of the TPM (see pages 9-10).

Regarding to claim 6, TCPA does not disclose wherein the network is the Internet. However, it is well known in the art that the customer can purchase products using credit card over the Internet (see details explanation in claims 1-2 above).

Claims 7-24 contain similar limitations found in claims 1-6 above, therefore, are rejected by the same rationale.

Regarding to claim 25, TCPA discloses a system comprising (see the entire document, pages 1-30):

a server (*see page 27, 2.12.2, Privacy CA*);

a customer computer including a TPM (*see page 27, 2.12.2, Owner)*;

a network linked to the server and the customer computer (*see page 15, an example of integrity mechanisms in a PC Subsystem, the application sent to network*);

first software stored in memory in the customer computer for requesting the TPM to create a TPM identity (*see page 27, 2.12.2, Owner)*;

second software stored in memory in the customer computer for obtaining a first certificate over the network from a CA (*see page 27, 2.12.2, Owner)*;

third software stored in memory in the customer computer for creating a non-migratable key (*see page 9, 2.5.1, the TPM contains a private endorsement key, the Owner makes available the endorsement credential the platform credential and the conformance credential)*;

sixth software stored in memory in the customer computer for sending to the server the TPM identity, the first certificate, and the non-migratable key (*see page 27, 2.12.2, Owner)*;

the server creating a public/private key pair and a second certificate (*see page 8, 2.4.1.7)*; and

the server sending the public/private key pair and the second certificate over the network to the customer computer (*see page 10)*.

TCPA does not disclose a server supporting a web site of a credit card company; fourth software stored in memory in the customer computer for browsing the web site of the credit card company over the network; fifth software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network. However, such features are well known in the art. For example, the conventional electronic commerce allows the user purchases products over the Internet using a credit card, the user having a computer system storing browser software, e.g. Netscape, Internet Explorer, can submits purchase request include credit card information, the credit card information is then transmitted to the credit card company having a web site for verifying and authorizing the purchase request. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to apply the method of TCPA above for the purpose improving the security in purchasing products using credit card over the Internet.

Claims 26-27 contain similar limitations found in claim 25 above, therefore, are rejected by the same rationale.

(10) Response to Argument

In response to appellant's argument regarding to claims 1, 2, 16 and 17 that TCPA does not teach "receiving from a customer over a network a non-migratable key, a first certificate by a TPM identify associated with a computer system used by the customer, second certificate acquired by the computer system from a certification authority", examiner submits that see page 9, section 2.5.1, the TPM contains a private endorsement key (a non-migratable key), the Owner makes available the endorsement credential the platform credential and the conformance credential (a first certificate by a TPM identify associated with a computer system used by the customer), and see page 7, 2.4.1.1 and 2.4.1.2, the CA enables determination of the identity of an entity by providing a certificate that binds the identity label of an entity (a second certificate acquired by the computer system from a Certification Authority (CA)).

In response to appellant's argument regarding to claims 1, 2, 16 and 17 that TCPA does not teach "creating a public/private key pair and a third certificate in response to the receiving step", examiner submits that *see page 8, 2.4.1.7*, TCPA discloses "Trusted Platform Module Entity" (3"PME) is the entity that vouches that a TPM is actually a TPM. *The TPME, and only the TPME, provides the root of the trust in the TPM.* The TPME causes an asymmetric key pair to exist in every TPM that it wishes to endorse. The public key of that key pair is the TPM's "public endorsement key." The TPME signs a credential containing the public endorsement key plus the statement "TCPA Trusted Platform Module Endorsement" and supplies that credential with the TPM that it wishes to endorse. This arrangement facilitates a defense to attacks in which a public key masquerades as the identity key of a Subsystem while in fact belonging to arbitrary hardware that does not satisfy the requirements placed upon a Subsystem.

In response to appellant's argument regarding to claims 1, 2, 16 and 17 that TCPA does not teach "sending the public/private key pair and the third certificate to the customer over the network", examiner submits that *see page 10*, TCPA discloses the process of sending the public/private key pair and the third certificate to the customer over the network.

In response to appellant's argument that regarding the well-known statement recited in rejecting claims 1, 2, 16 and 17, examiner submits that the appellant has not submitted any rebuttal of the well-known statement, the applicant has not presented arguments that the feature is not well known. The applicant only argued, "the applicant respectfully traverses and requests the Examiner to provide a reference that teaches receiving from a customer over a network an application for a credit card authorization." This does not constitute a proper challenge to the Official Notice.

In response to appellant's argument regarding to claims 3, 4, 18 and 19, examiner submits that TCPA further discloses wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity, wherein the third certificate is associated with an endorsement key of the TPM (see pages 9-10).

In response to appellant's argument regarding to claims 5 and 20, examiner submits that TCPA does not disclose wherein the network is the Internet. However, it is well known in the art that the customer can purchase products using credit card over the Internet (see details explanation in claims 1-2 above).

In response to appellant's argument regarding to claims 7-15 and 21-24, examiner submits that claims 7-24 contain similar limitations found in claims 1-6 above, therefore, are rejected by the same rationale.

In response to appellant's argument regarding to claims 25-27, examiner submits that the same explanations stated above in claims 1-6 applied for claims 25-27.

(11) Related Proceedings Appendix

The statement of the related proceedings appendix contained in the brief is correct.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Nga Nguyen

NGA NGUYEN
PRIMARY EXAMINER

Conferees

James Kramer

Frantzy Poinvil

WINSTEAD SECHREST & MINICK P.C.
P.O. BOX 50784
DALLAS, TEXAS 75201